UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/781,158	02/13/2001	Mikio Hashimoto	203056US2RD	9457

22850 7590 08/11/2004

OBLON, SPIVAK, MCCLELLAND, MAIER & NEUSTADT, P.C.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER	
NALVEN, ANDREW L	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 08/11/2004

12

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/781,158	HASHIMOTO ET AL.	
	Examiner	Art Unit	
	Andrew L Nalven	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 February 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9 and 12-20* is/are rejected.

7)☒ Claim(s) *10-11* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *13 February 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *1, 3, 7*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-20 are pending.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 1, 5, 6, 12-14, and 20 are rejected under 35 U.S.C. 102(b) as being anticipated by Arnold et al US Patent No. 4,558,176. Arnold discloses a computer system designed to inhibit unauthorized copying, usage, and cracking of protected software.

4. With regards to claims 1 and 14, Arnold teaches a reading unit configured to read out a plurality of programs encrypted by using different execution code encryption keys from an external memory (Arnold, column 5 lines 27-38, PUBRAN as reading unit), a decryption unit configured to decrypt the plurality of programs read out by the reading unit by using respective decryption keys (Arnold, column 4 lines 25-41, CPU), an execution unit configured to execute the plurality of programs decrypted by the decryption unit (Arnold, column 4 lines 25-41, CPU), a context information saving unit configured to save a context information for one program whose execution is to be interrupted, into the external memory or a context information memory provided inside

the microprocessor (Arnold, column 14 lines 5-19, ICM), the context information containing information indicating an execution state of the one program and the execution code encryption key of the one program (Arnold, column 14 lines 5-19, context and registers, columns 15/16 – Table II execution key register, column 7 lines 34-35), and a restart unit configured to restart an execution of the one program by reading out the context information from the external memory or the context information memory and recovering the execution state of the one program from the context information (Arnold, column 14 lines 36-46).

5. With regards to claim 5, Arnold teaches the context information saving unit being configured to save the context information in a plaintext form into the context information memory which is not readable by another program (Arnold, column 14 lines 5-19) and the restart unit configured to restart an execution of the one program by reading out the context information from the context information memory and receiving the execution state of the one program from the context information (Arnold, column 14 lines 36-46).

6. With regards to claim 6, Arnold teaches the restart unit restarting the execution of the one program in response to an execution of a prescribed instruction by another program (Arnold, column 14 lines 42-46, special instruction).

7. With regards to claim 12, Arnold teaches an execution state memory unit for storing an execution state of a currently executed program (Arnold, column 14 lines 5-19) and an execution state initialization unit configured to initialize a content of the execution state memory unit to a prescribed value or encrypts the content of the

execution state memory unit before an execution of another program starts after the one program is interrupt (Arnold, column 14 lines 12-14, initializing by altering all registers).

8. With regards to claim 13, Arnold teaches the key reading unit being configured to read out the execution code encryption key of each program that is encrypted by using the public key in advance, from the external memory (Arnold, column 5 lines 8-20), a key decryption unit configured to decrypt the execution code encryption key read out by the key reading unit by using the secret key (Arnold, column 5 lines 8-37), and wherein the decryption unit decrypts each program by using the execution code encryption key as a decryption key (Arnold, column 5 lines 8-37, column 4 lines 25-41).

9. With regards to claim 20, Arnold teaches the constituent elements of the microprocessor being contained in a single chip or a single package (Arnold, column 4 lines 25-33).

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. Claims 2-4, 7-9, 16-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Arnold et al US Patent No. 4,558,176 in view of Markus Kuhn "The TrustNo 1 Crypto processor Concept" and Bruce Schneier Applied Cryptography.

12. With regards to claims 2 and 7, Arnold fails to teach the information saving unit being configured to encrypt the context information using the public key and the saving of encrypted context information into the external memory and the restart unit configured to restart execution of one of the programs by reading out the encrypted context information from the external memory and decrypting the encrypted context information using the secret key thereby recovering the execution state. Kuhn teaches the information saving unit being configured to encrypt the context information using a key and the saving of encrypted context information into the external memory (Kuhn, page 3 column 2 paragraphs 1 and 3, SAVE_STATE) and the restart unit configured to restart execution of one of the programs by reading out the encrypted context information from the external memory and decrypting the encrypted context information using a key thereby recovering the execution state (Kuhn, page 3 column 2 paragraphs 1 and 3, RESTORE_STATE). Schneier teaches the encrypting of data with a public key and the subsequent decrypting of that data with a private key (Schneier, Section 2.5, Pages 31-32). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Kuhn's method of encrypting context information and Schneier's method of public key encryption with Arnold's secure computer system because it offers the advantage of allowing the storage of context information in a way that does not endanger confidentiality or integrity of the state of the process (Kuhn, page 3 column 2 paragraphs 1) and ensures that only the processor can decrypt the encrypted context information (Schneier, Section 2.5, Page 31).

13. With regards to claim 3, Arnold as modified teaches the restart unit restarting the execution of the one program only when a decrypted execution code encryption key contained in the decrypted context information coincides with the execution code encryption key of the one program (Kuhn, page 3 column 2 paragraph 3 and page 4 column 1 paragraph 1).

14. With regards to claim 4, Arnold as modified teaches the restart unit using a decrypted execution code encryption key contained in the decrypted context information as a decryption key for decrypting the one program (Arnold, column 5 lines 8-37, column 4 lines 25-41).

15. With regards to claim 8, Arnold as modified teaches all that is described above and further teaches the storing of the encrypted context information into an address on the external memory that is specified by another program (Kuhn, page 3 column 2 paragraph 1, "location that is specified as a parameter of the function").

16. With regards to claim 9, Arnold fails to teach the generating of a random number as a temporary key, the encrypting of the context information, the saving of encrypting context information into the external memory, the encrypted context information containing a first value obtained by encrypting information indicating the execution state of the one program by using the temporary key and a second value obtained by encrypting the temporary key with the public key, and the restart unit being configured to decrypt the temporary key from the second value contained in the encrypted context information indicating the execution state from the first value contained in the encrypted context information by using the decrypted temporary key. Kuhn teaches the

generating of a random number as a temporary key (Kuhn, Page 3, column 2 Paragraph 3, Hj), the encrypting of the context information (Kuhn, page 3 column 2 paragraphs 1 and 3, SAVE_STATE), the saving of encrypting context information into the external memory (Kuhn, page 3 column 2 paragraphs 1 and 3, SAVE_STATE), the encrypted context information containing a first value obtained by encrypting information indicating the execution state of the one program by using the temporary key (Kuhn, page 3 column 2 paragraph 3, encrypts both together with Hj), and the restart unit being configured to decrypt the temporary key from the second value contained in the encrypted context information indicating the execution state from the first value contained in the encrypted context information by using the temporary key (Kuhn, page 3 column 2 paragraph 3, decrypts with Hj). Schneier provides teaching for encrypting keys with a public key and decrypting keys with a private key (Scnneier, Page 48, Key Exhange with Public Key Cryptography). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Kuhn's method of encrypting context information and Schneier's method of public key encryption with Arnold's secure computer system because it offers the advantage of allowing the storage of context information in a way that does not endanger confidentiality or integrity of the state of the process (Kuhn, page 3 column 2 paragraphs 1) and ensures that only the processor can decrypt the encrypted context information (Schneier, Section 2.5, Page 31).

17. With regards to claim 16, Arnold teaches a cache memory for caching plaintext instructions and plaintext data for the plurality of programs in units of cache lines, the

cache memory having an attribute area for each cache line indicating a decryption key identifier for uniquely identifying a decryption key used in decrypting each program whose instructions are cached in each cache line or each program whose execution has caused caching of the plaintext data in each cache line (Kuhn, page 2 column 2 paragraph 3) and a cache access control unit configured to permit a data referring caused by an execution of one cached program stored in one cache line with respect to one cached data in another cache line only when the decryption key identifier indicated by the encryption attribute for the one cache line coincides with the decryption key identifier indicated by the encryption attribute for another cache line (Kuhn, page 3 column 1 paragraph 2).

18. With regards to claims 17-18, Arnold as modified teaches that when the data referring is not permitted, new data is cached into another cache line from the external memory (Kuhn, page 3 column 2 paragraph 3, "if the key indices do not match..cache line..reloaded").

19. Claims 15 is rejected under 35 U.S.C. 103(a) as being unpatentable over Arnold et al US Patent No. 4,558,176 in view of Bruce Schneier Applied Cryptography.

20. With regards to claim 15, Arnold teaches everything described above and further teaches a related information-writing unit for writing related information (Arnold, column 14 lines 5-35), a related information reading unit configured to read out the related information from the external memory according to an address of a data to be referred by the currently executed program (Arnold, column 14 lines 50-60), but fails to teach the

inclusion of a signature and the verification of the signature to determine if the signature contained in the field coincides with an original signature of the microprocessor. Schneier teaches the inclusion of signatures and the subsequent verification (Schneier, Section 2.6, Pages 34-35). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Schneier's signature method with Arnold's secure computing system because it offers the advantage of verifying that the signed data came from a trusted source and is unaltered (Schneier, Section 2.6, Page 34).

21. Claims 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Arnold et al US Patent No. 4,558,176 in view of Drake US Patent No. 6,006,328. Drake discloses a computer software authentication, protection, and security system.

22. With regards to claim 19, Arnold teaches the execution of plaintext programs (Arnold, column 4 lines 25-27), but fails to teach a debugging function that causes exceptions and that is invalidated during execution of a secure program. Drake teaches a debugging function that causes exceptions and that is invalidated during execution of a secure program (Drake, column 4 lines 48-60, column 6 line 51 – column 7 line 30). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Drake's method of preventing debugging during the execution of a secure program because it offers the advantage of helping prevent an attacker from tracing the execution of software in order to find vulnerabilities in its security (Drake, column 6 lines 51-57).

Allowable Subject Matter

23. Claims 10-11 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

24. The following is a statement of reasons for the indication of allowable subject matter: the cited prior art fails to specifically teach or suggest the context saving unit containing a third value obtained by encrypting the temporary key by using the execution code encryption key of the program. The cited prior art thus fails to anticipate or render the above limitations obvious.

Conclusion

25. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

26. Chorley et al US Patent No. 4,634,807 discloses a software protection device.

27. Allen et al US Patent No. 4,757,533 discloses a security system for microcomputers.

28. McCarty US Patent No. 5,666,411 discloses a system for computer software protection.

29. Cassagnol et al US Patent No. 6,385,727 discloses an apparatus for providing a secure processing environment.

30. England et al US Patent No. 6,651,171 discloses a system for secure execution of program code.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Andrew L Nalven whose telephone number is 703 305 8407. The examiner can normally be reached on Monday - Thursday 8-6, Alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on 703 308 4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Andrew Nalven

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100